HIPAA Security – Contingency Planning Guide for Information Technology Systems

NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology (IT) Systems* provides instructions, recommendations, and considerations for government IT contingency planning. Contingency planning refers to interim measures to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) from a variety of sources such as natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort, it is virtually impossible to completely eliminate all risks. In many cases, critical resources may reside outside the organization's control (such as electric power or telecommunications), and the organization may be unable to ensure their availability. Thus effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. Accordingly, in order for contingency planning to be successful agency management must ensure the following:

1. Understand the IT Contingency Planning Process and its place within the overall Continuity of Operations Plan and Business Continuity Plan process.

2. Develop or reexamine their contingency policy and planning process and apply the elements of the planning cycle, including preliminary planning, business impact analysis, alternate site selection, and recovery strategies.

3. Develop or reexamine their IT contingency planning policies and plans with emphasis on maintenance, training, and exercising the contingency plan. This document addresses specific contingency planning recommendations for seven IT platform types[1] and provides strategies and techniques common to all systems.

- Desktops and portable systems
- Servers
- Web sites
- Local area networks
- Wide area networks

- Distributed systems
- Mainframe systems.

[1] IT platforms or IT systems are considered any major application or general support system; the terms are used interchangeably.

The document also defines the following seven-step contingency process that an agency may apply to develop and maintain a viable contingency planning program for their IT systems. These seven progressive steps are designed to be integrated into each stage of the system development life cycle.

1. **Develop the contingency planning policy statement.** A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan.

2. **Conduct the business impact analysis (BIA).** The BIA helps to identify and prioritize critical IT systems and components. A template for developing the BIA is also provided to assist the user.

3. **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

4. **Develop recovery strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

5. **Develop an IT contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system.

6. **Plan testing, training, and exercises.** Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.

7. **Plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements.

The document presents a sample format for developing an IT contingency plan. The format defines three phases that govern the actions to be taken following a system disruption. The **Notification/Activation** Phase describes the process of notifying recovery personnel and performing a damage assessment. The **Recovery** Phase discusses a suggested course of action for recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities. The final phase, **Reconstitution**, outlines actions that can be taken to return the system to normal operating conditions.